UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/773,089	02/03/2004	Andrew Dellow	851963.415	3294

38106 7590 03/27/2007

SEED INTELLECTUAL PROPERTY LAW GROUP PLLC
701 FIFTH AVENUE, SUITE 5400
SEATTLE, WA 98104-7092

EXAMINER	
AHUJA, SUPRIYA	
ART UNIT	**PAPER NUMBER**
2109	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/27/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/773,089	DELLOW, ANDREW	
	Examiner	Art Unit	
	Supriya Ahuja	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 February 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☒ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Oath/Declaration

1. It does not identify the mailing address of each inventor. A mailing address is an address at which an inventor customarily receives his or her mail and may be either a home or business address. The mailing address should include the ZIP Code designation. The mailing address may be provided in an application data sheet or a supplemental oath or declaration. See 37 CFR 1.63(c) and 37 CFR 1.76.

2. It does not identify the foreign application for patent or inventor's certificate on which priority is claimed pursuant to 37 CFR 1.55, and any foreign application having a filing date before that of the application on which priority is claimed, by specifying the application number, country, day, month and year of its filing.

3. It does not identify the city and either state or foreign country of residence of each inventor. The residence information may be provided on either an application data sheet or supplemental oath or declaration.

Drawings

4. New corrected drawing in compliance with 37 CFR 1.121(d) is required in this application because in Fig. 1, the central processing unit (CPU) is missing the reference no. 21 in the specification ([0026] line 1). Applicant is advised to employ the services of a competent patent draftsperson outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office action to

avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

Specification

5. The disclosure is objected to because of the following informalities:

On Page 9, line 6, the word "multiplexors" should be replaced by --multiplexers--.

Appropriate correction is required.

Claim Objections

6. **Claims 1-29, 30-34 and 36-37** are objected to because of the following informalities:

In claim 1 line 11, the phrase "provides data" should be replaced by --provides the data--.

In claim 3, line 2, the phrase "plurality of possible rule signals" is objected to because "rule signals" lacks antecedent basis and needs to be corrected appropriately for using the word "possible".

In claim 7, line 2, the phrase "an instruction" should be replaced by --the instruction--.

In claim 18, line 3, the phrase "cryptographic circuit (9)" should be replaced with --cryptographic circuit--.

In claim 26, line 2, the word "multiplexor" should be replaced by --multiplexer--.

In claims 28 and 29, line 2, the phrase "the encryption system" lacks antecedent basis and should be replaced --an encryption system--.

In claim 30, line 3 the phrase "select routing" should be replaced by --select the routing--.

In claim 31, line 4, the phrase "the plurality of data" lacks antecedent basis and should be replaced by --a plurality of data--.

In claim 32, line 5, the phrase "the encryption/decryption circuits" lacks antecedent basis and should be corrected appropriately.

In claim 33, line 1, the phrase "a plurality of anti-fuses" should be replaced by --the plurality of anti-fuses--.

In claim 36, line 15, the phrase "the output" should be replaced by --an output-- and line 18, the phrase "a key" should be replaced by --the key--.

Claims 2, 4-6, 8-17, 19-25, 27, 34, and 37 are rejected for being dependent upon rejected base claims 1, 32 and 36.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. **Claims 1-29 and 36-37** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

In claim 1, line 13, the phrase "it operates in accordance" is not accepted and is not in accordance with legal claim writing, as the word "it" is very unclear as to what it is referring to and therefore, should be corrected appropriately.

In claim 1 line 8, the phrase "an instruction interpreter" is confusing as it is unclear in the specification as to what the instruction interpreter is in the circuit. Similar problem exists for claims 2, 27 and 36.

In claim 4, line 1, the phrase "the rule signal" is confusing as it is unclear as to which rule signal its referring to with respect to the plurality of possible rule signals in claim 3.

Claims 2-3, 5-29 and 37 are rejected for being dependent upon rejected base claims 1 and 36.

Appropriate corrections are required.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. **Claims 1 and 36** are rejected under 35 U.S.C. 103(a) as being unpatentable over Tozawa et al. (US 2003/0159062 dated 08/21/2003) in view of Taylor (US 5313590 dated 05/17/1994), Ash et al. (US 5559877 dated 09/24/1996), and Baba (US 5432949 dated 07/11/1995).

Towaza et al. discloses a cryption/decryption communication semiconductor device comprising one or two or more encryption/decryption circuits (cryptographic circuit), which encrypt or decrypt input data in accordance with a predetermined algorithm and a plurality of external interfaces for performing the input/output of data from and to external devices. The communication interface, the encryption/decryption circuits and the plurality of external interfaces are formed on one semiconductor chip. In the cryption and decryption communication semiconductor device, input data sent from any one of the plurality of external interfaces is encrypted or decrypted by at least one of the encryption/decryption circuits and is

capable of being outputted to any different one of the plurality of external interfaces (abstract). Towaza et al further discloses an encrypt/decrypt processor comprising an encryption/decryption circuit, an input selection which selects input of data inputted to the encryption/decryption circuit from the processing circuit, an output selector which selects the output of data outputted from the encryption/decryption circuit to the packet processing circuit [0039]. Moreover, a system control device made up of CPU is the like is disclosed, which signals for controlling the link and packet processing circuit, the cryption and decryption communication semiconductor device using a key, etc. [0041].

Towaza et al. discloses all the limitations of claims 1 and 36 accept it does not disclose the cryptographic circuit in a semiconductor integrated circuit, which selectively receives input from multiple sources. Towaza et al. also does not disclose a rule selection circuit using a rule selection scheme and an instruction interpreter configured to receive instruction signal and generate an output signal.

The general concept of using a plurality of sources and destinations coupled via a plurality of data pathways is well known in the art as illustrated by Taylor which discloses a data routing circuitry designed for routing data from a selected source processor element to a selected destination processor element manufactured on a single integrated chip (col.1 lines 55 – 60).

The general concept of a rule selection circuit is well known in the art as illustrated by Ash et al. which discloses a rule-based end-to-end routing scheme, which automatically selects a routing path from multiple candidates based on class-of-service parameters and availability of network capacity (abstract) using selection switches.

The general concept of using an instruction interpreter in a encryption/decryption circuit is well known in the art as illustrated by Baba which discloses an instruction decoder (interpreter) configured to receive the routing rule and the instruction signal and generate an output signal (col. 3 lines 50-60).

It would have been obvious to one in ordinary skill in the art at the time of the invention was made to modify Towaza et al. to include the use of a data routing circuitry as illustrated by Taylor in order to have multiple options.

It would have been obvious to one in ordinary skill in the art at the time of the invention was made to modify Towaza et al. to include the use of a rule selection circuit as illustrated by Ash et al. in order to select rules using switches.

It would have been obvious to one in ordinary skill in the art at the time of the invention was made to modify Towaza et al. to include the use of a instruction interpreter as illustrated by Baba in order to generate output signal to be encrypted or decrypted.

11. **Claims 2 and 3** are rejected under 35 U.S.C. 103(a) as being unpatentable over Tozawa et al. (US 2003/0159062 dated 08/21/2003), Taylor (US 5313590 dated 05/17/1994), Ash et al. (US 5559877 dated 09/24/1996), and Baba (US 5432949 dated 07/11/1995) and in further view of Staver (US 5650951 dated 07/22/1997).

Tozawa et al., Taylor, Ash et al., and Baba disclose all the limitations of claims 2 and 3 except that the instruction interpreter receives signals that are unselect-able chosen from a plurality of rule signals according to a mode of operation of the system. The general concept of receiving signals that are unselect-able according to a mode of operation is well known in the art as illustrated by Staver which discloses a programmable data acquisition system including a

plurality of input channels for receiving a respective input signal during a normal mode of operation. Staver also discloses individual test circuits are used for selecting respective ones of the plurality of channels to receive predetermined reference signals during a test mode of operation while uninterruptedly providing normal mode of operation in any remaining unselected channels in the acquisition system (abstract). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Tozawa et al., Taylor, Ash et al., and Baba to include the use of receiving signals that are unselect-able according to a mode of operation as illustrated by Staver as an obvious signal selecting technique in order to select the rule signals.

12. **Claims 4 and 5** are rejected under 35 U.S.C. 103(a) as being unpatentable over Tozawa et al. (US 2003/0159062 dated 08/21/2003), Taylor (US 5313590 dated 05/17/1994), Ash et al. (US 5559877 dated 09/24/1996), Baba (US 5432949 dated 07/11/1995) and Staver (US 5650951 dated 07/22/1997) and in further view of Lien et al. (US 6301696 dated 10/09/2001).

Tozawa et al., Taylor, Ash et al., Baba and Staver disclose all the limitations of claims 4 and 5 except the rule signal is generated by a rule selector comprising of a plurality of anti-fuses where each of the anti-fuses can be configured once only. The general concept of using anti-fuses to select configurations is well known in the art as illustrated by Lien et al. which discloses a method of making an integrated chip including an initial design for a field-programmable gate array (FPGA) which employs fuses or anti-fuses as switches to select cell functions or connections, which means that each FPGA IC can be programmed only once (col. 1 lines 52-65). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Tozawa et al., Taylor, Ash et al., Baba and Staver to include the use of anti-fuses as

illustrated by Lien et al in order to provide higher density and smaller or more predictable delays as stated by Lien et al. (col. 1 lines 65-67).

13. **Claims 6 and 7** are rejected under 35 U.S.C. 103(a) as being unpatentable over Tozawa et al. (US 2003/0159062 dated 08/21/2003), Taylor (US 5313590 dated 05/17/1994), Ash et al. (US 5559877 dated 09/24/1996), and Baba (US 5432949 dated 07/11/1995) and in further view of Kimura (US 5093819 dated 03/03/1992).

Tozawa et al., Taylor, Ash et al., and Baba disclose all the limitations of claims 6 and 7 except the CPU generates the instruction signal comprising of an instruction portion and a data portion. The general concept of a CPU generating an instruction signal with two portions is well known in the art as illustrated by Kimura which discloses CPU outputting a write instruction to the disk drive and transferring a data portion signal to the disc driver (col. 6 lines 24-29). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Tozawa et al., Taylor, Ash et al., and Baba to include the use of an instruction signal generated by a CPU as illustrated by Kimura in order to execute instructions by the CPU.

14. **Claim 8** is rejected under 35 U.S.C. 103(a) as being unpatentable over Tozawa et al. (US 2003/0159062 dated 08/21/2003), Taylor (US 5313590 dated 05/17/1994), Ash et al. (US 5559877 dated 09/24/1996), and Baba (US 5432949 dated 07/11/1995) and in further view of Alves et al. (US 2003/0007636 dated 01/09/2003).

Tozawa et al., Taylor, Ash et al., and Baba disclose all the limitations of claim 8 except that the instruction signal and the rule signal are 32-bit data fields. The general concept of using a 32-bit data signal is well known in the art as illustrated by Alves et al. which discloses the core processor is 32-bit which communicates with the external memory through a 32-bit data bus

(Page 1 [0014]). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Tozawa et al., Taylor, Ash et al., and Baba to include the use of a 32-bit data signal as an obvious signal choice in order to store to signal in a compact size as disclosed by Alves et al. [0014].

15. **Claim 9** is rejected under 35 U.S.C. 103(a) as being unpatentable over Tozawa et al. (US 2003/0159062 dated 08/21/2003), Taylor (US 5313590 dated 05/17/1994), Ash et al. (US 5559877 dated 09/24/1996), and Baba (US 5432949 dated 07/11/1995) and in further view of Zeidler (US 4423287 dated 12/27/1983).

Tozawa et al., Taylor, Ash et al., and Baba disclose all the limitations of claim 9 except that the encryption/decryption keys are stored in a memory. The general concept of storing keys in a memory is well known in the art as illustrated by Zeidler which discloses source and destination terminals storing master keys in the terminals memory (col. 3 lines 49 – 61). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Tozawa et al., Taylor, Ash et al., and Baba to include the use of a memory to store the keys in order to provide storage for keys to be retrieved later.

16. **Claims 10-12** are rejected under 35 U.S.C. 103(a) as being unpatentable over Tozawa et al. (US 2003/0159062 dated 08/21/2003), Taylor (US 5313590 dated 05/17/1994), Ash et al. (US 5559877 dated 09/24/1996), and Baba (US 5432949 dated 07/11/1995) and in further view of Saunders (US 6209099 dated 03/27/2001).

Tozawa et al., Taylor, Ash et al., and Baba disclose all the limitations of claims 10-12 except that the there exists a key store. The general concept of having a key store is well known in the art as illustrated by Saunders, which discloses a security circuit having a cryptographic engine and a

cryptographic key store, which stores keys (col. 1 lines 35-50). This is an intrinsic property of the key store that keys are selected from the key store based on some sort of signal or instruction or algorithm and are provided to the key input according to the algorithm or conditions or selected path. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Tozawa et al., Taylor, Ash et al., and Baba to include the use of a key store as illustrated by Saunders in order to store keys to generate a digital signature as disclosed by Saunders (col. 1 lines 55-60).

17. **Claims 13-15** are rejected under 35 U.S.C. 103(a) as being unpatentable over Tozawa et al. (US 2003/0159062 dated 08/21/2003), Taylor (US 5313590 dated 05/17/1994), Ash et al. (US 5559877 dated 09/24/1996), and Baba (US 5432949 dated 07/11/1995) further in view of Candelore (WO 00/59222 dated 10/05/2000).

Tozawa et al., Taylor, Ash et al., and Baba disclose all the limitations of claims 13-15 except that the circuit descrambles television broadcast signals using control words and encrypted control words are decrypted using service key, where the service key is decrypted using a secret key. The general concept of using control words and keys to descramble the television broadcasting signals is well known in the art as illustrated by Candelore which discloses descrambling digital content using control words, where the control words are decrypted using service keys and the service keys are decrypted using unique keys or secret keys (page 9 lines 1-7, page 11 lines 1-10, page 12 lines 1-7, page 16 lines 3-5). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Tozawa et al., Taylor, Ash et al., and Baba to include the use of encrypted words and keys to descramble digital content in order to provide grant access to the paid content to authorized users as disclosed by Candelore (page 3 lines 20-23).

18. **Claim 16** is rejected under 35 U.S.C. 103(a) as being unpatentable over Tozawa et al. (US 2003/0159062 dated 08/21/2003), Taylor (US 5313590 dated 05/17/1994), Ash et al. (US 5559877 dated 09/24/1996), and Baba (US 5432949 dated 07/11/1995) further in view of Bayle (5416916 dated 05/16/1995).

Tozawa et al., Taylor, Ash et al., and Baba disclose all the limitations of claim 16 except that the circuit is arranged to perform memory-to-memory transfers. The general concepts of using memory-to-memory transfers in an integrated circuit is well known in the art as illustrated by Bayle which discloses an integrated circuit temporarily storing data only during a direct memory-to-memory transfer operation (claim 1 col. 5 lines 4-7). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Tozawa et al., Taylor, Ash et al., and Baba to include the use of memory-to-memory transfers as illustrated by Bayle in order to store data (col. 5 lines 5-8).

19. **Claims 17-20** are rejected under 35 U.S.C. 103(a) as being unpatentable over Tozawa et al. (US 2003/0159062 dated 08/21/2003), Taylor (US 5313590 dated 05/17/1994), Ash et al. (US 5559877 dated 09/24/1996), Baba (US 5432949 dated 07/11/1995) and Saunders (US 6209099 dated 03/27/2001) further in view of Candelore (WO 00/59222 dated 10/05/2000).

Tozawa et al., Taylor, Ash et al., Baba and Saunders disclose all the limitations of claims 17-20 except that the data is a key (It is factual that data can be in any form such as a key which is generated by a software and is an obvious generation technique which is well known in the art), data source and destination is a memory storing control words, keys or the broadcast data. The general concept of using a memory to store data, where data can be in any form- a key generated by a software, control words or a signal is well known in the art as illustrated Candelore which

discloses key stored in memory (col. 9 lines 1-5). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Tozawa et al., Taylor, Ash et al., Baba and Saunders to include the use of memory to store data, where data can be in any form as illustrated by Candelore as an obvious storage technique.

20. **Claims 21-23** are rejected under 35 U.S.C. 103(a) as being unpatentable over Tozawa et al. (US 2003/0159062 dated 08/21/2003), Taylor (US 5313590 dated 05/17/1994), Ash et al. (US 5559877 dated 09/24/1996), Baba (US 5432949 dated 07/11/1995) and Zeidler (US 4423287 dated 12/27/1983) and further in view of Candelore (WO 00/59222 dated 10/05/2000). Tozawa et al., Taylor, Ash et al., Baba and Zeidler disclose all the limitations of claims 21-23 except that one of the key memories stores a key for decrypting other keys or control words. The general concept of storing a key (It is factual that the key can be generated using a software algorithm and is an obvious key-generation technique) in a memory to decrypt data (It is factual that data can be in the form of a service key or a control word) is well known in the art as illustrated by Candelore which discloses key stored in a memory or register where that key is a service key used to decrypt control words and store secret key or unique key used to decrypt service key (claims 5 and 25, page 9 lines 1-7, page 11 lines 1-10, page 12 lines 1-7, page 16 lines 3-5). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Tozawa et al., Taylor, Ash et al., Baba and Zeidler to include the use of a memory to store keys in order to decrypt control words and keys as illustrated by Candelore (claims 5 and 25).

21. **Claims 24 and 26** are rejected under 35 U.S.C. 103(a) as being unpatentable over Tozawa et al. (US 2003/0159062 dated 08/21/2003), Taylor (US 5313590 dated 05/17/1994),

Ash et al. (US 5559877 dated 09/24/1996), and Baba (US 5432949 dated 07/11/1995) and further in view of Rangasayee (US 6356108 dated 03/12/2002).

Tozawa et al., Taylor, Ash et al., and Baba disclose all the limitations of claims 24 and 26 except that the data sources and destinations includes at least one of a hard disc, ROM, RAM, data in port and data out port where the plurality of selectable pathways are selected by at least one multiplexer or switch. The general concept of using a switch or a multiplexer to select between different data sources and data destinations which includes ports is well known in the art as illustrated by Rangasayee which discloses ATM switches utilizing separate and distinct memory arrays at both the source ports and destination ports (col. 7 lines 33 – 37). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Tozawa et al., Taylor, Ash et al., and Baba to include the use of a switch to select pathways between source ports and destination ports as illustrated by Rangasayee in order to select pathways.

22. **Claim 25** is rejected under 35 U.S.C. 103(a) as being unpatentable over Tozawa et al. (US 2003/0159062 dated 08/21/2003), Taylor (US 5313590 dated 05/17/1994), Ash et al. (US 5559877 dated 09/24/1996), and Baba (US 5432949 dated 07/11/1995) and further in view of Snell (US 2003/0223580 dated 12/04/2003).

Tozawa et al., Taylor, Ash et al., and Baba disclose all the limitations of claim 25 except that the cryptographic circuit is an AES circuit. The general concept of using an AES circuit as a cryptographic circuit is well known in the art as illustrated by Snell, which discloses a cryptographic engine that may be an application-specific integrated circuit (ASIC) designed to carry out the AES operation (Page 3 [0035]). It would have been obvious to one of ordinary skill

in the art at the time of the invention to modify Tozawa et al., Taylor, Ash et al., and Baba to include the use of a AES circuit as illustrated by Snell as an obvious design choice.

23. **Claim 27** is rejected under 35 U.S.C. 103(a) as being unpatentable over Tozawa et al. (US 2003/0159062 dated 08/21/2003), Taylor (US 5313590 dated 05/17/1994), Ash et al. (US 5559877 dated 09/24/1996), and Baba (US 5432949 dated 07/11/1995) and further in view of Lamiaux (US 4155118 dated 05/15/1979).

Tozawa et al., Taylor, Ash et al., and Baba disclose all the limitations of claim 27 except that the instruction interpreter comprises a plurality of combinatorial components arranged such that the output is generated as a function of the instruction signal. The general concept of the instruction interpreter having a plurality of combinatorial components (It is factual for a interpreter to be made up of a combinations of components) where the output is a function of the instruction signal (The output is always dependent on the input signal in this case the instruction signal and therefore is a function of the instruction signal) is well known in the art as illustrated by Lamiaux which discloses the single chip controller comprising an arithmetic logic unit and a plurality of active storage elements all interconnected in parallel via an input bus and an output bus (abstract). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Tozawa et al., Taylor, Ash et al., and Baba to include the use of output generated as a function of the instruction signal generated by the instruction interpreter in order to create an output signal based on the input signal.

24. **Claim 28** are rejected under 35 U.S.C. 103(a) as being unpatentable over Tozawa et al. (US 2003/0159062 dated 08/21/2003), Taylor (US 5313590 dated 05/17/1994), Ash et al. (US

5559877 dated 09/24/1996), and Baba (US 5432949 dated 07/11/1995) and further in view of Candelore (WO 00/59222 dated 10/05/2000).

Tozawa et al., Taylor, Ash et al., and Baba disclose all the limitations of claim 28 except that the encryption system is a subscriber-based pay-television system. The general concept of using a semiconductor integrated system in a subscriber based pay-television system is well known in the art as illustrated by Candelore which discloses an apparatus for descrambling digital content in digital devices with a Pay-TV access control application (col. 1 lines 14-16, col. 1 lines 45 – 55). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Tozawa et al., Taylor, Ash et al., and Baba to include the use of a semiconductor integrated circuit in a pay-television system as an obvious design choice.

25. **Claim 29** are rejected under 35 U.S.C. 103(a) as being unpatentable over Tozawa et al. (US 2003/0159062 dated 08/21/2003), Taylor (US 5313590 dated 05/17/1994), Ash et al. (US 5559877 dated 09/24/1996), and Baba (US 5432949 dated 07/11/1995).

Tozawa et al., Taylor, Ash et al., and Baba disclose all the limitations of claim 29 where the encryption system in the semiconductor integrated circuit is a monolithic integrated circuit (Baba, title, and col. 1 lines 50-55).

26. **Claim 37** is rejected under 35 U.S.C. 103(a) as being unpatentable over Tozawa et al. (US 2003/0159062 dated 08/21/2003), Taylor (US 5313590 dated 05/17/1994), Ash et al. (US 5559877 dated 09/24/1996), and Baba (US 5432949 dated 07/11/1995) and further in view of Candelore (WO 00/59222 dated 10/05/2000).

Tozawa et al., Taylor, Ash et al., and Baba disclose all the limitations of claim 37 except cryptographic circuit includes encrypted control words and a service key. The general concept

of using a key from the instruction signal to decrypt the service key and thereafter decrypt the encrypted control words in accordance with the decrypted service key is well known in the art as illustrated by Candelore which discloses receiving an encrypted control word in the descrambler integrated circuit, which is decrypted using a service key (page 12 line 5) stored in a register circuit of the descrambler integrated circuit, descrambling the digital content using the decrypted control word (abstract). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Tozawa et al., Taylor, Ash et al., and Baba to include the use of encrypted control words and a service key as illustrated by Candelore in order to decrypt the secure digital content to be viewed by the subscriber.

27. **Claim 30** is rejected under 35 U.S.C. 103(a) as being unpatentable over Ash et al. (US 5559877 dated 09/24/1996) and further in view of Lien et al. (US 6301696 dated 10/09/2001). Ash et al. discloses all the limitations of claim 30 except that the rule signal is generated by a rule selector comprising of a plurality of anti-fuses where each of the anti-fuses can be configured once only. The general concept of using anti-fuses to select configurations is well known in the art as illustrated by Lien et al. which discloses a method of making an integrated chip including an initial design for a field-programmable gate array (FPGA) which employs fuses or anti-fuses as switches to select cell functions or connections, which means that each FPGA IC can be programmed only once (col. 1 lines 52-65). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Ash et al. to include the use of anti-fuses as illustrated by Lien et al in order to provide higher density and smaller or more predictable delays as stated by Lien et al. (col. 1 lines 65-67).

28. **Claim 31** is rejected under 35 U.S.C. 103(a) as being unpatentable over Tozawa et al. (US 2003/0159062 dated 08/21/2003), Kimura (US 5093819 dated 03/03/1992) and Baba (US 5432949 dated 07/11/1995).

Towaza et al. discloses a cryption/decryption communication semiconductor device comprising one or two or more encryption/decryption circuits, which encrypt or decrypt input data in accordance with a predetermined algorithm and a plurality of external interfaces for performing the input/output of data from and to external devices. The communication interface, the encryption/decryption circuits and the plurality of external interfaces are formed on one semiconductor chip. In the cryption and decryption communication semiconductor device, input data sent from any one of the plurality of external interfaces is encrypted or decrypted by at least one of the encryption/decryption circuits and is capable of being outputted to any different one of the plurality of external interfaces (abstract). Towaza et al further discloses an encrypt/decrypt processor comprising an encryption/decryption circuit, an input selection which selects input of data inputted to the encryption/decryption circuit from the processing circuit, an output selector which selects the output of data outputted from the encryption/decryption circuit to the packet processing circuit [0039]. Moreover, a system control device made up of CPU is the like is disclosed, which signals for controlling the link and packet processing circuit, the cryption and decryption communication semiconductor device using a key, etc. [0041].

Tozawa et al. discloses all the limitations of claim 31 except generating of the instruction signal comprising of an instruction portion and a data portion. The general concept of a CPU generating an instruction signal with two portions is well known in the art as illustrated by Kimura which discloses CPU outputting a write instruction to the disk drive and transferring a

data portion signal to the disc driver (col. 6 lines 24-29). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Tozawa et al. to include the use of an instruction signal generated by a CPU as illustrated by Kimura in order to execute instructions by the CPU.

Towaza et al. and Kimura disclose all the limitations of claim 31 except for an instruction interpreter configured to receive instruction signal and generate an output signal. The general concept of using an instruction interpreter in a encryption/decryption circuit is well known in the art as illustrated by Baba which discloses an instruction decoder (interpreter) configured to receive the routing rule and the instruction signal and generate an output signal (col. 3 lines 50-60). It would have been obvious to one in ordinary skill in the art at the time of the invention was made to modify Towaza et al. and Kimura to include the use of an instruction interpreter as illustrated by Baba in order to generate output signal to be encrypted or decrypted.

29. **Claim 32** are rejected under 35 U.S.C. 103(a) as being unpatentable over Tozawa et al. (US 2003/0159062 dated 08/21/2003) in view of Taylor (US 5313590 dated 05/17/1994), Ash et al. (US 5559877 dated 09/24/1996), and Baba (US 5432949 dated 07/11/1995).

Towaza et al. discloses a cryption/decryption communication semiconductor device comprising one or two or more encryption/decryption circuits, which encrypt or decrypt input data in accordance with a predetermined algorithm and a plurality of external interfaces for performing the input/output of data from and to external devices. The communication interface, the encryption/decryption circuits and the plurality of external interfaces are formed on one semiconductor chip. In the cryption and decryption communication semiconductor device, input data sent from any one of the plurality of external interfaces is encrypted or decrypted by

at least one of the encryption/decryption circuits and is capable of being outputted to any different one of the plurality of external interfaces (abstract). Towaza et al further discloses an encrypt/decrypt processor comprising an encryption/decryption circuit, an input selection which selects input of data inputted to the encryption/decryption circuit from the processing circuit, an output selector which selects the output of data outputted from the encryption/decryption circuit to the packet processing circuit [0039]. Moreover, a system control device made up of CPU is the like is disclosed, which signals for controlling the link and packet processing circuit, the cryption and decryption communication semiconductor device using a key, etc. [0041].

Towaza et al. discloses all the limitations of claim 32 accept it does not disclose the cryptographic circuit in a semiconductor integrated circuit, which selectively receives input from multiple sources. Towaza et al. also does not disclose a rule selection circuit using a rule selection scheme and an instruction interpreter configured to receive instruction signal and generate an output signal.

The general concept of a plurality of sources and destinations coupled via a plurality of data pathways is well known in the art as illustrated by Taylor which discloses a data routing circuitry designed for routing data from a selected source processor element to a selected destination processor element manufactured on a single integrated chip (col.1 lines 55 – 60).

The general concept of a rule selection circuit is well known in the art as illustrated by Ash et al. which discloses a rule-based end-to-end routing scheme, which automatically selects a routing path from multiple candidates based on class-of-service parameters and availability of network capacity (abstract) using selection switches.

The general concept of using an instruction interpreter in a encryption/decryption circuit is well known in the art as illustrated by Baba which discloses an instruction decoder (interpreter) configured to receive the routing rule and the instruction signal and generate an output signal (col. 3 lines 50-60).

It would have been obvious to one in ordinary skill in the art at the time of the invention was made to modify Towaza et al. to include the use of a data routing circuitry as illustrated by Taylor in order to have multiple options.

It would have been obvious to one in ordinary skill in the art at the time of the invention was made to modify Towaza et al. to include the use of a rule selection circuit as illustrated by Ash et al. in order to select rules using switches.

It would have been obvious to one in ordinary skill in the art at the time of the invention was made to modify Towaza et al. to include the use of a instruction interpreter as illustrated by Baba in order to generate output signal to be encrypted or decrypted.

30. **Claim 33** is rejected under 35 U.S.C. 103(a) as being unpatentable over Tozawa et al. (US 2003/0159062 dated 08/21/2003) in view of Taylor (US 5313590 dated 05/17/1994), Ash et al. (US 5559877 dated 09/24/1996), Baba (US 5432949 dated 07/11/1995) and in further view of Lien et al. (US 6301696 dated 10/09/2001).

Tozawa et al., Taylor, Ash et al., and Baba disclose all the limitations of claim 33 except the rule signal is generated by a rule selector comprising of a plurality of anti-fuses where each of the anti-fuses can be configured once only. The general concept of using anti-fuses to select configurations is well known in the art as illustrated by Lien et al. (US 6301696 dated 10/09/2001) which discloses a method of making an integrated chip including an initial design

for a field-programmable gate array (FPGA) which employs fuses or anti-fuses as switches to select cell functions or connections, which means that each FPGA IC can be programmed only once (col. 1 lines 52-65). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Tozawa et al., Taylor, Ash et al., and Baba to include the use of anti-fuses as illustrated by Lien et al in order to provide higher density and smaller or more predictable delays as stated by Lien et al. (col. 1 lines 65-67).

31. **Claim 34** is rejected under 35 U.S.C. 103(a) as being unpatentable over Tozawa et al. (US 2003/0159062 dated 08/21/2003), Taylor (US 5313590 dated 05/17/1994), Ash et al. (US 5559877 dated 09/24/1996), and Baba (US 5432949 dated 07/11/1995) and in further view of Candelore (WO 00/59222 dated 10/05/2000).

Tozawa et al., Taylor, Ash et al., and Baba disclose all the limitations of claim 34 except that the circuit descrambles television broadcast signals using control words and encrypted control words are decrypted using service key, where the service key is decrypted using a secret key. The general concept of using control words and keys to descramble the television broadcasting signals is well known in the art as illustrated by Candelore which discloses descrambling digital content using control words, where the control words are decrypted using service keys and the service keys are decrypted using unique keys or secret keys (page 9 lines 1-7, page 11 lines 1-10, page 12 lines 1-7, page 16 lines 3-5). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Tozawa et al., Taylor, Ash et al., and Baba to include the use of encrypted words and keys to descramble digital content in order to provide grant access to the paid content to authorized users as disclosed by Candelore (page 3 lines 20-23).

32. **Claim 35** are rejected under 35 U.S.C. 103(a) as being unpatentable over Tozawa et al. (US 2003/0159062 dated 08/21/2003) in view of Taylor (US 5313590 dated 05/17/1994), Ash et al. (US 5559877 dated 09/24/1996), Baba (US 5432949 dated 07/11/1995), Kimura (US 5093819 dated 03/03/1992), Zeidler (US 4423287 dated 12/27/1983) and Candelore (WO 00/59222 dated 10/05/2000).

Towaza et al. discloses a cryption/decryption communication semiconductor device comprising one or two or more encryption/decryption circuits, which encrypt or decrypt input data in accordance with a predetermined algorithm and a plurality of external interfaces for performing the input/output of data from and to external devices. The communication interface, the encryption/decryption circuits and the plurality of external interfaces are formed on one semiconductor chip. In the cryption and decryption communication semiconductor device, input data sent from any one of the plurality of external interfaces is encrypted or decrypted by at least one of the encryption/decryption circuits and is capable of being outputted to any different one of the plurality of external interfaces (abstract). Towaza et al further discloses an encrypt/decrypt processor comprising an encryption/decryption circuit, an input selection which selects input of data inputted to the encryption/decryption circuit from the processing circuit, an output selector which selects the output of data outputted from the encryption/decryption circuit to the packet processing circuit [0039]. Moreover, a system control device made up of CPU is the like is disclosed, which signals for controlling the link and packet processing circuit, the cryption and decryption communication semiconductor device using a key, etc. [0041].

Towaza et al. discloses a cryption/decryption communication semiconductor device comprising one or two or more encryption/decryption circuits (cryptographic circuit), which encrypt or

decrypt input data in accordance with a predetermined algorithm and a plurality of external interfaces for performing the input/output of data from and to external devices. The communication interface, the encryption/decryption circuits and the plurality of external interfaces are formed on one semiconductor chip. In the cryption and decryption communication semiconductor device, input data sent from any one of the plurality of external interfaces is encrypted or decrypted by at least one of the encryption/decryption circuits and is capable of being outputted to any different one of the plurality of external interfaces (abstract). Towaza et al further discloses an encrypt/decrypt processor comprising an encryption/decryption circuit, an input selection which selects input of data inputted to the encryption/decryption circuit from the processing circuit, an output selector which selects the output of data outputted from the encryption/decryption circuit to the packet processing circuit [0039]. Moreover, a system control device made up of CPU is the like is disclosed, which signals for controlling the link and packet processing circuit, the cryption and decryption communication semiconductor device using a key, etc. [0041].

Towaza et al. discloses all the limitations of claims 35 accept it does not disclose the cryptographic circuit in a semiconductor integrated circuit, which selectively receives input from multiple sources. Towaza et al. also does not disclose a rule selection circuit using a rule selection scheme and an instruction interpreter configured to receive instruction signal and generate an output signal. Moreover, Tozawa et al. does not disclose that the CPU generates the instruction signal comprising of an instruction portion and a data portion and that the encryption/decryption keys are stored in a memory. In addition, Tozawa et al. does not disclose that the circuit descrambles television broadcast signals using control words and encrypted

control words are decrypted using service key, where the service key is decrypted using a secret key.

The general concept of a plurality of sources and destinations coupled via a plurality of data pathways is well known in the art as illustrated by Taylor which discloses a data routing circuitry designed for routing data from a selected source processor element to a selected destination processor element manufactured on a single integrated chip (col.1 lines 55 – 60).

The general concept of a rule selection circuit is well known in the art as illustrated by Ash et al. which discloses a rule-based end-to-end routing scheme, which automatically selects a routing path from multiple candidates based on class-of-service parameters and availability of network capacity (abstract) using selection switches.

The general concept of using an instruction interpreter in a encryption/decryption circuit is well known in the art as illustrated by Baba which discloses an instruction decoder (interpreter) configured to receive the routing rule and the instruction signal and generate an output signal (col. 3 lines 50-60).

The general concept of a CPU generating an instruction signal with two portions is well known in the art as illustrated by Kimura which discloses CPU outputting a write instruction to the disk drive and transferring a data portion signal to the disc driver (col. 6 lines 24-29).

The general concept of storing keys in a memory is well known in the art as illustrated by Zeidler which discloses source and destination terminals storing master keys in the terminals memory (col. 3 lines 49 – 61).

The general concept of using control words and keys to descramble the television broadcasting signals is well known in the art as illustrated by Candelore which discloses descrambling digital

content using control words, where the control words are decrypted using service keys and the service keys are decrypted using unique keys or secret keys (page 9 lines 1-7, page 11 lines 1-10, page 12 lines 1-7, page 16 lines 3-5).

It would have been obvious to one in ordinary skill in the art at the time of the invention was made to modify Towaza et al. to include the use of a data routing circuitry as illustrated by Taylor in order to have multiple options.

It would have been obvious to one in ordinary skill in the art at the time of the invention was made to modify Towaza et al. to include the use of a rule selection circuit as illustrated by Ash et al. in order to select rules using switches.

It would have been obvious to one in ordinary skill in the art at the time of the invention was made to modify Towaza et al. to include the use of a instruction interpreter as illustrated by Baba in order to generate output signal to be encrypted or decrypted.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Tozawa et al. to include the use of an instruction signal generated by a CPU as illustrated by Kimura in order to execute instructions by the CPU.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Tozawa et al. to include the use of a memory to store the keys in order to provide storage for keys to be retrieved later.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Tozawa et al. to include the use of encrypted words and keys to descramble digital content in order to provide grant access to the paid content to authorized users as disclosed by Candelore (page 3 lines 20-23).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Supriya Ahuja whose telephone number is 571-270-1588. The examiner can normally be reached on Monday - Thursday 7:30 -5:00; 2nd Friday 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Frantz Jules can be reached on 571-272-1808. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Supriya Ahuja

S.A.
March 14, 2007

FRANTZ JULES
SUPERVISORY PATENT EXAMINER